



# UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE  
United States Patent and Trademark Office  
Address: COMMISSIONER FOR PATENTS  
P.O. Box 1450  
Alexandria, Virginia 22313-1450  
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/649,755	08/26/2003	James N. Guichard	CIS03-34(7598)	7343
22468 7590 02/21/2007 CHAPIN & HUANG L.L.C. WESTBOROUGH OFFICE PARK 1700 WEST PARK DRIVE WESTBOROUGH, MA 01581			EXAMINER TRAN, ELLEN C	
			ART UNIT 2134	PAPER NUMBER

SHORTENED STATUTORY PERIOD OF RESPONSE	MAIL DATE	DELIVERY MODE
3 MONTHS	02/21/2007	PAPER

**Please find below and/or attached an Office communication concerning this application or proceeding.**

If NO period for reply is specified above, the maximum statutory period will apply and will expire 6 MONTHS from the mailing date of this communication.

<b>Office Action Summary</b>	<b>Application No.</b>		<b>Applicant(s)</b>	
	10/649,755		GUICHARD ET AL.	
	<b>Examiner</b>		<b>Art Unit</b>	
	Ellen C. Tran		2134	

**-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --**

**Period for Reply**

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

**Status**

- 1) ☒ Responsive to communication(s) filed on 26 August 2003.
- 2a) ☐ This action is **FINAL**.                      2b) ☒ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

**Disposition of Claims**

- 4) ☒ Claim(s) 1-45 is/are pending in the application.
- 4a) Of the above claim(s) \_\_\_\_\_ is/are withdrawn from consideration.
- 5) ☐ Claim(s) \_\_\_\_\_ is/are allowed.
- 6) ☒ Claim(s) 1-45 is/are rejected.
- 7) ☐ Claim(s) \_\_\_\_\_ is/are objected to.
- 8) ☐ Claim(s) \_\_\_\_\_ are subject to restriction and/or election requirement.

**Application Papers**

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☐ The drawing(s) filed on \_\_\_\_\_ is/are: a) ☐ accepted or b) ☐ objected to by the Examiner.  
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).  
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

**Priority under 35 U.S.C. § 119**

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All    b) ☐ Some \*    c) ☐ None of:
1. ☐ Certified copies of the priority documents have been received.
2. ☐ Certified copies of the priority documents have been received in Application No. \_\_\_\_\_.
3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

\* See the attached detailed Office action for a list of the certified copies not received.



**Attachment(s)**

- |  |   |
|--|---|
| 1) <input checked="" type="checkbox"/> Notice of References Cited (PTO-892)  | 4) <input type="checkbox"/> Interview Summary (PTO-413)<br>Paper No(s)/Mail Date. _____ |
| 2) <input type="checkbox"/> Notice of Draftsperson's Patent Drawing Review (PTO-948)   | 5) <input type="checkbox"/> Notice of Informal Patent Application                       |
| 3) <input checked="" type="checkbox"/> Information Disclosure Statement(s) (PTO/SB/08)<br>Paper No(s)/Mail Date <u>13 May 2004</u> . | 6) <input type="checkbox"/> Other: _____  |

***DETAILED ACTION***

1. This action is responsive to communication: original application filed on 26 August 2003.
2. Claims 1-45 are currently pending in this application. Claims 1, 11, 21, 31, and 41-45 are independent claims.
3. The IDS submitted 13 May 2004 has been considered.

***Claim Rejections - 35 USC § 103***

4. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

5. **Claims 1-4, 6-14, and 16-45**, are rejected under 35 U.S.C. 103(a) as being unpatentable over Casey et al. U.S. Patent 6,205,488 (hereinafter '488) in view of Ginger et al. US Patent No. 6,751,729 (hereinafter '729).

**As to independent claim 1, "In a first node of a physical network supporting multiple virtual network connections, a method to dynamically modify configuration data supporting virtual networks, the method comprising:"** is taught in '488 col. 1, line 61 through col. 2, line 10";

**"generating a notification message including the network address information and the corresponding gateway identifier; and transmitting the notification message to a second node of the physical network enabling the second node to establish a virtual network**

Art Unit: 2134

**connection between the second node and the first node on which to forward data messages to the at least one host computer based on the corresponding gateway identifier”** is shown in ‘488 col. 4, lines 31-46;

the following is not explicitly taught in ‘488: **“receiving i) network address information associated with at least one host computer, and ii) a corresponding gateway identifier of a gateway in the physical network”** however ‘729 teaches accepting an identification of a server and an address on the data network of the server during configuring and authenticating a node device, in col. 5, lines 44-49, note the server is considered equivalent to the gateway.

It would have been obvious to one of ordinary skill in the art at the time of the invention a virtual private network enabled to dynamically distribute VPN information taught in ‘488 to include a means to utilize address and server identification information. One of ordinary skill in the art would have been motivated to perform such a modification because a means is needed to save cost when establishing multiple VPNs see ‘789 (col. 1, lines 33 et seq.) “An important impetus for the adoption of VPN technology by businesses is the significant cost saving associated with the replacement of expensive remote access servers and associated long distance dial-up charges, the substitution of inexpensive and ubiquitous Internet access for expensive leased lines and frame relay access, and the introduction of a flexible, fast, secure, and inexpensive mechanism for exchanging data with suppliers and customers”. In addition all prior art references are related to the same field of endeavor VPNs and the use of edge routers.

**As to dependent claim 2, “wherein generating a notification message further comprises: generating at least a portion of the notification message in accordance with a distribution protocol utilized by service providers to disseminate routing policy**

Art Unit: 2134

**information to customer edge nodes; and wherein transmitting a notification message includes: transmitting the network address information and the corresponding gateway identifier as an appendix to the notification message”** is taught in ‘488 col. 3, lines 1-11.

**As to dependent claim 3, “wherein the distribution protocol is based at least in part on an interautonomous system routing protocol and the virtual network connection between the second node and the first node is a virtual private network connection overlaid on the physical network, one end of the virtual private network connection terminating at the gateway identified by the corresponding gateway identifier”** is shown in ‘488 col. 3, lines 12-22.

**As to dependent claim 4, “further comprising: transmitting routing policy attribute information in addition to the network address information and corresponding gateway identifier to the second node to more particularly define a policy for routing the data messages on a corresponding virtual network connection through the gateway to the at least one host computer”** however ‘729 teaches that policys are distributed in col. 2, lines 55-58. The motivation to combine ‘488 and ‘729 is the same as stated above in claim 1.

**As to dependent claim 6, “wherein transmitting the network address and identifier includes: delivering the notification message including the network address and corresponding gateway identifier to multiple customer edge nodes of the physical network, each customer edge node updating its corresponding configuration data for establishing private networks between the customer edge nodes based on the network address and corresponding gateway identifier”** however ‘729 teaches that broadcast messages are sent to

Art Unit: 2134

other nodes devices updating them on the changes to configuration in col. 2, line 64 through col. 3, line 6. The motivation to combine '488 and '729 is the same as stated above in claim 1.

**As to dependent claim 7, “wherein the first and second nodes are customer edge nodes in a network and the network supports virtual private networks terminating at the customer edge nodes”** however '729 teaches customer edge nodes in col. 1, lines 13-15.

**As to dependent claim 8, “wherein the network address information identifies a single host computer”** however '729 teaches a computer identification in col. 7, lines 53-58.

**As to dependent claim 9, “wherein the network address information identifies a range of host computers that are part of a network coupled to the first node”** however '729 teaches a range addresses in col. 8, lines 53-67. The motivation to combine '488 and '729 is the same as stated above in claim 1.

**As to dependent claim 10, “wherein the corresponding gateway identifier is an IPsec identity associated with the at least one host computer”** however '729 teaches IPsec in col. 2, lines 28-31. The motivation to combine '488 and '729 is the same as stated above in claim 1.

**As to independent claim 11,** this claim is directed to the computer system of the method of claim 1; therefore it is rejected along similar rationale.

**As to dependent claims 12-14, and 16-20,** these claims contain substantially similar subject matter as claims 2-4 and 6-10; therefore they are rejected along similar rationale.

**As to independent claim 21, “In a receiving node of a physical network supporting multiple virtual network connections, a method to dynamically modify configuration data associated with at least one of the multiple virtual network connections, the method comprising:”** is taught in '488 col. 1, line 61 through col. 2, line 10”;



**“and based on contents of the notification message, modifying a map at the receiving node to include the network address information and configuration data identifying at least part of a virtual network connection between the receiving node and the sending node on which to forward data messages through the gateway to a destination node”** is shown in ‘488 col. 3, lines 38-54;

the following is not explicitly taught in ‘488: **“receiving a notification message from a sending node of the physical network, the notification message including network address information and a corresponding gateway identifier of a gateway of the physical network”** however ‘729 teaches accepting an identification of a server and an address on the data network of the server during configuring and authenticating a node device, in col. 5, lines 44-49, note the server is considered equivalent to the gateway.

It would have been obvious to one of ordinary skill in the art at the time of the invention a virtual private network enabled to dynamically distribute VPN information taught in ‘488 to include a means to utilize address and server identification information. One of ordinary skill in the art would have been motivated to perform such a modification because a means is needed to save cost when establishing multiple VPNs see ‘789 (col. 1, lines 33 et seq.) “An important impetus for the adoption of VPN technology by businesses is the significant cost saving associated with the replacement of expensive remote access servers and associated long distance dial-up charges, the substitution of inexpensive and ubiquitous Internet access for expensive leased lines and frame relay access, and the introduction of a flexible, fast, secure, and inexpensive mechanism for exchanging data with suppliers and customers”. In addition all prior art references are related to the same field of endeavor VPNs and the use of edge routers.

**As to dependent claim 22, “further comprising: upon forwarding data messages through the receiving node, utilizing the map to identify on which virtual network to forward the data messages through the gateway to the destination node” is taught in ‘488 col. 4, lines 51-67**

**As to dependent claim 23, “further comprising: at the receiving node including the map, receiving a data message to be forwarded based on a corresponding destination address; comparing the destination address and a source address of the data message to network address information stored in the map; identifying, based on the destination address, how to transmit the data message to the destination node based on a corresponding virtual network connection specified in the map” is shown in ‘488 col. 4, lines 51-67.**

**As to dependent claim 24, “further comprising: in response to identifying that the destination address of the data message matches network address information in the map, establishing the corresponding virtual network connection specified in the map on which to transmit the data message to the destination node” is disclosed in ‘488 col. 4, lines 51-67.**

**As to dependent claim 25, “wherein establishing a virtual network connection includes establishing a virtual private network connection between the receiving node and sending node based on IKE (Internet Key Exchange) protocol and IPsec (Internet Protocol Security)” however ‘729 teaches IPsec in col. 2, lines 28-31 and ‘729 teaches IKE in col. 15, lines 23-34. The motivation to combine ‘488 and ‘729 is the same as stated above in claim 21.**

**As to dependent claim 26, “further comprising: in response to identifying that the destination address of the data message matches network address information in the map,**



**identifying whether a corresponding virtual network connection specified in the map has been established and, if so, transmitting the data message on the established virtual network connection to the destination node”** is taught in ‘488 col. 4, lines 16-30.

As to dependent claim 27, **“wherein the network address information identifies a single host computer”** however ‘729 teaches IPsec in col. 2, lines 28-31. The motivation to combine ‘488 and ‘729 is the same as stated above in claim 21.

As to dependent claim 28, **“wherein the network address information identifies a range of host computers that are part of a network coupled to the first node”** however ‘729 teaches a range addresses in col. 8, lines 53-67. The motivation to combine ‘488 and ‘729 is the same as stated above in claim 21.

As to dependent claim 29, **“wherein the corresponding gateway identifier is an IPsec identity associated with the at least one host computer”** however ‘729 teaches IPsec in col. 2, lines 28-31. The motivation to combine ‘488 and ‘729 is the same as stated above in claim 21.

As to dependent claim 30, **“wherein the gateway is located in the sending node”** however ‘729 teaches that a server, i.e. gateway can be coupled to a node device in col. 3, lines 7-16. The motivation to combine ‘488 and ‘729 is the same as stated above in claim 21.

As to independent claim 31, this claim is directed to the computer system of the method of claim 21; therefore it is rejected along similar rationale.

As to dependent claims 32-40, these claims contain substantially similar subject matter as claims 22-30; therefore they are rejected along similar rationale.

As to independent claim 41, this claim is directed to a computer program performing the method of claim 1; therefore it is rejected along similar rationale.

**As to independent claim 42**, this claim is a means claim performing the method of claim 1; therefore it is rejected along similar rationale. The means to perform the method is shown in the above rejection.

**As to independent claim 43**, this claim is directed to a computer program performing the method of claim 21; therefore it is rejected along similar rationale.

**As to independent claim 44**, this claim is a means claim performing the method of claim 21; therefore it is rejected along similar rationale. The means to perform the method is shown in the above rejection.

**As to independent claim 45**, this claim is directed to customer edge routers that incorporates substantially similar subject matter of the methods of claims 1 and 21; therefore it is rejected along similar rationale.

6. **Claims 5, and 15**, are rejected under 35 U.S.C. 103(a) as being unpatentable over Casey et al. U.S. Patent 6,205,488 (hereinafter '488) in view of Ginger et al. US Patent No. 6,751,729 (hereinafter '729 in further view of Simon et al. US Patent No. 7,028,183 (hereinafter '183).

**As to dependent claim 5**, the following is not taught in the combination of '488 and '729: **"wherein the first and the second nodes are part of a network that does not inherently support encryption services and configuration data at the second node at least partially supports encryption of data messages forwarded to the at least one host computer through the gateway identified by the corresponding gateway identifier"** however '183 teaches "Whereas the embodiments which have been described are directed toward relocating the IKE negotiation procedure, in yet another embodiment, the IPsec (AH or ESP protocol) processing is

Art Unit: 2134

moved. This IPsec processing may be located in a node referred to herein as an encryption node or in any one of a plurality of encryption nodes, where the encryption node(s) may be physically separate from the edge routers. Packet filters within the edge routers control which traffic from the end nodes must pass to these encryption nodes and which traffic may pass directly (and therefore without encryption through the IPsec tunnel) to the destination hosts. In some configurations, these packet filters therefore can reduce the amount of traffic that must pass through the encryption nodes, thereby reducing the overall cryptographic load. This is in contrast to the prior art, in which the end node either transmits all data through the IPsec tunnel or in which the end node is solely responsible for selecting which traffic passes through the IPsec tunnel encryption. In particular, the packet filters within the edge routers enable the network to enforce cryptographic policies without relying on the proper configuration of the end nodes. In this embodiment, the encryption nodes may be co-located with cryptographic node processing thus providing the functionality of a conventional IPsec endpoint” in col. 9, lines 21-45.

It would have been obvious to one of ordinary skill in the art at the time of the invention a virtual private network enabled to dynamically distribute VPN information taught in ‘488 and ‘729 to include a means to use nodes that do not inherently support encryption. One of ordinary skill in the art would have been motivated to perform such a modification because of the complexity introduced by a wireless environment see ‘183 (col. 4, lines 6 et seq.) “A particular difficulty for a distributed or clustered IPsec implementation is distribution of cipher keys. Two serious problems arise. First, for IKE negotiation to succeed, all of the IKE packets for establishing the SA must arrive at the same physical node (e.g. edge router); otherwise no SA will be negotiated and no encrypted traffic can ever be exchanged. This presents a problem with

Art Unit: 2134

mobile devices, which may be passed from one edge router to another during the time that an IKE negotiation process is underway. Second, once IKE negotiation has produced one or more SAs, those SAs must be made available to every node (e.g. edge router) that can transmit or receive traffic using the associated IP address. That is, the SAs (and their associated cipher keys, ESP parameters, and AH parameters) need to be available at any edge router to which a mobile wireless end node's traffic is directed, in order for the collection of edge routers to provide seamless yet secure connectivity for the mobile end node. Otherwise, packets may arrive at nodes at which they cannot be decrypted /encrypted or authenticated, resulting in severe problems including significant packet loss and communication breakdown, and in turn, an increase in network latency and a decrease in network throughput".

As to dependent claim 15, this claim contains substantially similar subject matter as claim 5; therefore it is rejected along similar rationale.

### ***Conclusion***

7. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Ellen C Tran whose telephone number is

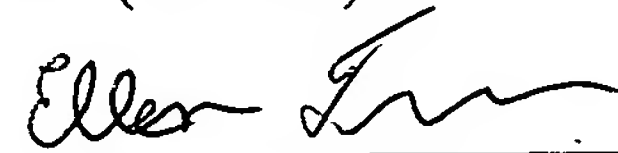
(571) 272-3842. The examiner can normally be reached from 6:00 am to 4:00 pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kambiz Zand can be reached on (571) 272-3811. The fax phone number for the organization where this application or proceeding is assigned is (571) 273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished

Art Unit: 2134

applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).



---

Ellen Tran  
Patent Examiner  
Technology Center 2134  
15 February 2007